(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日:
2003年9月18日(18.09.2003)

PCT

(10) 国际公布号:
WO 03/077467 A1

(51) 国际分类号[7]: H04L 9/00

(21) 国际申请号: PCT/CN03/00106

(22) 国际申请日: 2003年1月30日(30.01.2003)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
02110974.5 2002年3月8日(08.03.2002) CN

(71) 申请人(对除美国以外的所有指定国): 华为技术有限公司(HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市南山区科技园科发路华为用户服务中心大厦, Guangdong 518057 (CN)。

(72) 发明人;及
(75) 发明人/申请人(仅对美国): 李永茂(LI, Yongmao) [CN/CN]; 吴更石(WU, Gengshi) [CN/CN]; 中国广东省深圳市南山区科技园科发路华为用户服务中心大厦, Guangdong 518057 (CN)。

(74) 代理人: 上海专利商标事务所(SHANGHAI PATENT & TRADEMARK LAW OFFICE); 中国上海市桂平路435号, Shanghai 200233 (CN)。

(81) 指定国(国家): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW

(84) 指定国(地区): ARIPO专利(GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚专利(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲专利(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI专利(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

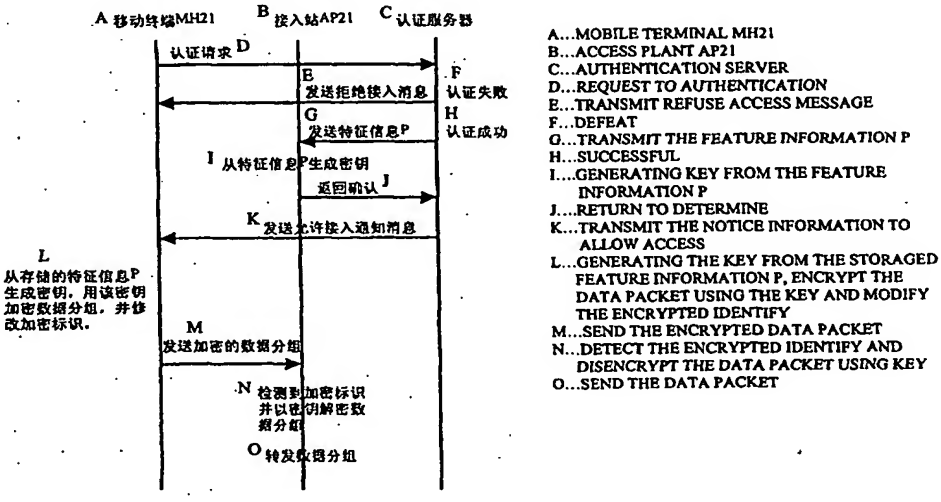
根据细则4.17的声明:
— 关于申请人在国际申请日有权申请并被授予专利(细则4.17(ii))对除美国以外的所有指定国
— 关于申请人在国际申请日有权要求该在先申请的优先权(细则4.17(iii))对除美国以外的所有指定国
— 发明人资格(细则4.17(iv))仅对美国

本国际公布:
— 包括国际检索报告。

所引用双字母代码和其它缩写符号，请参考刊登在每期PCT公报期刊起始的"代码及缩写符号简要说明"。

(54) Title: THE METHOD FOR DISTRIBUTES THE ENCRYPTED KEY IN WIRELESS LAN

(54) 发明名称: 无线局域网加密密钥的分发方法



(57) Abstract: An method for distributes the encrypted key in wireless LAN, this method combines the distribution course of the key with authentication course of the mobile terminal, utilizes the authentication server or the wireless gateway to manage the distribution of the key, so mobile terminal users may be roam in range greater than the range of the key manage server covers. Because the distribution of the key does not involve transmitting the key, which was not encrypted through the air interface, the method has ensured that the key is safe. In addition, the above-mentioned key distribution method does not depend on the specific authentication, therefore can use it under various kinds of authentication agreements. Finally, because AP does not need to manage user's information, the method simplified the structure of AP thus lowered costs.

[见续页]

WO 03/077467 A1

(57) 摘要

一种无线局域网加密密钥分发方法，该方法将密钥的分发过程与移动终端的认证过程结合在一起，利用认证服务器或无线网关对密钥分发进行管理，因此，移动终端用户可以在大于密钥管理服务器覆盖范围内跨区漫游。由于密钥的分发不涉及通过空中接口中传递未加密的密钥，所以保证了密钥安全。此外，上述密钥分配方法不依赖于特定的认证方式，因而可以在各种认证协议下实现。最后，由于 AP 无需管理用户信息，简化了 AP 的结构从而降低了成本。

无线局域网加密密钥的分发方法

发明领域

本发明涉及无线局域网内接入站(AP)与移动终端之间的通信，特别涉及加密密钥的分发方法。

背景技术

无线局域网借助无线信道传输数据、话音和视频信号。相对于传统布线网络，无线局域网具有安装便捷、使用灵活、经济节约和易于扩展等优点，因而日益受到重视。

无线局域网的可覆盖区域称为服务区域，一般分为基本服务区域(Basic Service Area，以下简称为 BSA)和扩展服务区域(Extended Service Area，以下简称为 ESA)，其中 BSA 指由无线局域网中各单元的无线收发机以及地理环境所确定的通信覆盖区域，常称为小区(cell)，范围一般较小；为了扩大无线局域网覆盖区域，通常采用如图 1 所示的方法，即通过接入站(Access Point，以下简称为 AP)经无线网关将 BSA 与骨干网(通常是有线局域网)相连接，使多个 BSA 中的移动终端 MH 经由 AP 和无线网关与有线骨干网连接，从而构成扩展服务区域。

与有线传输相比，无线传输的保密性较差，因此为了保证小区内 AP 与移动终端之间的通信安全，信息必须用密钥加密以后才能发送。当移动终端跨区移动或加电启动时，首先应寻找自己所在的小区，向该小区的 AP 登录，并获得该小区的相关信息，因此其与 AP 的加密通信将受到一定的限制。具体而言，例如当移动终端 MH12 从小区 1 进入小区 2 时，如果 AP11 与 AP21 属于同一密钥管理服务器的覆盖范围，则移动终端 MH12 与 AP11 的加密通信可以顺利过渡至其与 AP21 的加密通信而不受影响，但是如果 AP11 与 AP21 分属不同的密钥管理服务器，则由于 AP21 无法获知移动终端 MH12 的通信密钥，所以无法在小区 2 内直接实现移动终端 MH12 与 AP21 的加密通信。而如果由移动终端 MH12 将密钥以非加密方式通过无线信道发送给 AP21 来实现加密通信，则由于密钥容易被截获和破译，所以系统存在很大的安全隐患。

由上可见，现有技术下加密密钥的分发方法存在移动终端跨区漫游时加密通信受到限制的缺点。

发明内容

针对上述情况，本发明提出一种新的无线局域网加密密钥的分发方法。

按照本发明的无线局域网加密密钥的分发方法，所述无线局域网包含一接入站(AP)和若干存储自身标识信息的移动终端，移动终端通过无线信道与 AP

通信，AP 与外部网络和对移动终端身份进行认证的认证装置连接，所述认证装置存储有各移动终端的标识信息，所述方法包含如下步骤：

(1)移动终端向认证装置发送包含标识信息的认证请求以请求对其进行身份认证；

(2)认证装置根据认证请求中包含的标识信息对移动终端进行认证，如果认证失败，则经 AP 向移动终端发送拒绝接入消息；如果认证成功，则认证装置向 AP 发送与密钥有关的信息 M1，并且经 AP 向该移动终端发送包含允许接入通知信息的消息，如果该消息包含与密钥有关的信息 M2，则必须经过加密处理；

(3)AP 根据认证装置向其发送的与密钥有关的信息 M1 获得密钥，移动终端根据认证装置经 AP 向其发送的消息获得密钥。

由上可见，本发明的利用密钥的通信方法将密钥的分发过程与移动终端的认证过程结合在一起，利用认证装置对密钥分发进行管理，因此，移动终端用户可以在大于密钥管理服务器覆盖范围内跨区漫游。由于密钥的分发不涉及通过空中接口中传递未加密的密钥，所以保证了密钥安全。此外，上述密钥分配方法不依赖于特定的认证方式，因而可以在各种无线局域网协议下实现。最后，由于 AP 无需管理用户信息，简化了 AP 的结构从而降低了成本。

附图说明

通过以下结合附图对本发明实施例的描述，可以进一步理解本发明的各种优点、特点和特征，其中：

图 1 为无线局域网经 AP 和无线网关与有线骨干网连接的示意图；

图 2a 为按照本发明一个实施例的无线局域网内加密通信方法的示意图；

图 2b 为按照本发明另一实施例的无线局域网内加密通信方法的示意图；

图 2c 为按照本发明另一实施例的无线局域网内加密通信方法的示意图；

图 2d 为按照本发明另一实施例的无线局域网内加密通信方法的示意图；

图 3a 示出了无线局域网内动态协商密钥的一个实例过程；

图 3b 示出了无线局域网内动态协商密钥的另一个实例过程；

图 3c 示出了无线局域网内动态协商密钥的另一个实例过程；

图 3d 示出了无线局域网内动态协商密钥的另一个实例过程；以及

具体实施方式

以下首先借助图 1、图 2a－2d 描述按照本发明实施例的无线局域网内加密密钥的分发方法。

如图 1 所示，小区 1~3 包含一接入站 AP11、AP21 和 AP31 以及若干移动

终端 MH12~MH33，每个移动终端都存储有标识其身份的身份信息 I 和特征信息 P，每个移动终端通过无线信道与同属一个小区内的 AP 通信，AP 经无线网关 51-53 与有线骨干网 4 连接，骨干网内的认证服务器(未画出)包含了所有小区内的所有移动终端的身份信息 I 和特征信息 P，认证服务器也可以从外部设备获得存储每个移动终端身份信息 I 和特征信息 P 的用户列表，因此可以利用其存储的或用户列表提供的身份信息 I 对任一移动终端用户的身份进行确认。值得指出的是，移动终端的身份信息 I 和特征信息 P 也可以由无线网关 51-53 存储或管理，由此可由无线网关实现对移动终端用户身份的认证功能。另外，还可以由认证服务器与无线网关协同实现对移动终端用户身份的确认功能。对于本领域内的技术人员来说，实现移动终端用户的身份确认功能的方式是公知的并且可以有多种，利用认证服务器和/或无线网只是其中的几种方式，为方便表述起见，以下将具有移动终端用户身份确认功能的装置统称为认证装置。

图 2a 示出了移动终端 MH12 从小区 1 进入小区 2 时其与 AP21 之间通信用密钥的首次分发过程和加密通信过程。

移动终端 MH12 首先与 AP21 建立初始连接，经 AP21 和无线网关 51 向骨干网 4 内的认证服务器发送包含身份信息的认证请求以请求对其进行认证。认证服务器在接收到认证请求后，首先根据认证请求中包含的身份信息 I 对移动终端的身份进行认证，如果发现所包含的身份信息 I 与其存储的不相符，则判断移动终端用户为非法用户，认证请求无效，因此经无线网关 51 和 AP21 向移动终端 MH11 发送拒绝接入消息。如果发现认证请求所包含的身份信息 I 与其存储的相符，则判断移动终端用户为合法用户，认证请求有效，因此如图 2a 所示，认证服务器根据包含的身份信息 I 查找对应移动终端 MH12 的特征信息 P 并将查找到的特征信息 P 经无线网关 51 发送给 AP21。AP21 在接收到认证服务器发送的特征信息 P 之后经无线网关向认证服务器返回确认收到特征信息 P 的确认消息并根据密钥生成算法从特征信息 P 生成密钥。密钥生成算法可以是任意一种算法，并且密钥的长度是任意的。认证服务器在接收到 AP21 发送的确认消息之后即经无线网关 51 和 AP21 向移动终端 MH21 发送允许接入通知消息。移动终端 MH21 收到允许接入通知消息之后，根据与 AP21 生成密钥时所用的相同算法，从其自身存储的特征信息 P 生成密钥以用该密钥对发送至 AP21 的数据分组进行加密并向 AP21 发送，移动终端 MH21 在对数据分组进行加密时在数据分组内加入加密标识。AP21 在收到移动终端 MH21 发送的数据分组后，首先检测数据分组中的加密标识，如果检测到加密标识，则使用根据密钥生成算法从特征信息 P 得到的密钥对数据分组解密并经无线网关 51 转发至外部网络 4，否则将数据分组经无线网关 51 直接转发外部网络 4。

图 2b 为按照本发明另一实施例的无线局域网内加密通信方法的示意图。该实施例与图 2a 所示实施例的区别在于，在上述通信过程中，密钥由 AP21 利用任一密钥生成算法生成并用特征信息 P 对密钥加密后发送给移动终端 MH21。移动终端 MH21 在接收到 AP21 发送的密钥之后，用其自身存储的特征信息 P 对密钥进行解密，然后用解密后的密钥对发送至 AP 的数据分组进行加密并向 AP 发送，移动终端在对数据分组进行加密时在数据分组内也加入加密标识。在这种情况下，各移动终端无需知晓 AP21 所采用的密钥生成算法。

图 2c 为按照本发明另一实施例的无线局域网内加密通信方法的示意图。该实施例与图 2a 所示实施例的区别在于，当认证成功时，认证服务器可以根据密钥生成算法从查找到的特征信息 P 生成密钥并发送给 AP21 而不是将特征信息 P 发送给 AP21 供其生成密钥。

图 2d 为按照本发明另一实施例的无线局域网内加密通信方法的示意图。该实施例与图 2c 所示实施例的区别在于，当认证成功时，认证服务器可以根据密钥生成算法生成密钥并发送给 AP21，与此同时认证服务器还向移动终端 MH21 发送以特征信息 P 加密的密钥。

值得指出的是，骨干网 4 内可以包含若干台认证服务器，它们之间通过一定的通信协议连接以交换所存储的移动终端的标识信息，因此可以进一步扩大扩展服务区域。

在上述实施例中，如果移动终端用户身份的确认功能由无线网关 51－53 单独实现，则原先认证服务器所实现的其它功能也可以由无线网关实现，例如可以由无线网关 51－53 向移动终端 MH21 发送允许接入通知，生成密钥以及向 AP21 发送特征信息 P 等。同样，如果确认功能由认证服务器与无线网关协同实现，则原先认证服务器所实现的其它功能可以由认证服务器与无线网关协同实现。总之，原先认证服务器所实现的全部功能都可以由认证装置实现。

在上述无线局域网内加密通信过程中，为了进一步提高系统的安全性，AP 与移动终端之间的通信密钥还可定期或不定期动态更新。以下借助图 3a－3d 描述这种动态协商密钥的几个实例过程。

如图 3a 所示，为了更换密钥，首先由 AP 产生一个随机数，并利用任一密钥生成算法从该随机数生成密钥，随后 AP 将该随机数放入改变密钥通知一起发送给移动终端。当移动终端收到改变密钥通知后，就根据改变密钥通知中包含的随机数，利用相同的密钥生成算法产生密钥，随后用该密钥对发送至 AP 的数据分组进行加密并向 AP 发送，移动终端在对数据分组进行加密时仍在数据分组内加入加密标识并改变加密标识的数值以表示已经更换通信密钥。

图 3b 示出了另一动态协商密钥的实例过程，在图 3b 中，为了更换密钥，

首先由 AP 以任意方式生成新的密钥，随后 AP 用当前密钥对新生成的密钥进行加密并将加密后的密钥放入改变密钥通知一起发送给移动终端。当移动终端收到改变密钥通知后，用当前密钥解密包含在改变密钥通知中的新密钥，随后用该新密钥对发送至 AP 的数据分组进行加密并向 AP 发送，移动终端在对数据分组进行加密时仍在数据分组内加入加密标识并改变加密标识的数值以表示已经更换通信密钥。

图 3c 示出了另一动态协商密钥的实例过程，在图 3c 中，为了更换密钥，首先由认证装置产生一个随机数，并利用任一密钥生成算法从该随机数生成密钥，随后认证装置将该随机数发送给移动终端并将生成的密钥发送给 AP。当 AP 收到认证装置发送的密钥之后，向移动终端发送改变密钥通知。当移动终端收到改变密钥通知和随机数后，利用相同的密钥生成算法产生密钥，随后用该密钥对发送至 AP 的数据分组进行加密并向 AP 发送，移动终端在对数据分组进行加密时仍在数据分组内加入加密标识并改变加密标识的数值以表示已经更换通信密钥。

图 3d 示出了另一动态协商密钥的实例过程，在图 3d 中，为了更换密钥，首先由认证装置以任意方式生成新的密钥，随后认证装置将密钥发送给 AP 并用当前密钥对新生成的密钥进行加密后发送给移动终端。AP 在接收到认证装置发送的未加密密钥后向移动终端发送改变密钥通知。当移动终端收到改变密钥通知和加密的密钥后，用当前密钥解密加密密钥以得到新密钥，随后用该新密钥对发送至 AP 的数据分组进行加密并向 AP 发送，移动终端在对数据分组进行加密时仍在数据分组内加入加密标识并改变加密标识的数值以表示已经更换通信密钥。

在上述动态协商密钥过程中，如果 AP 在发出改变密钥通知以后，发现移动终端发送的数据分组内加密标识的数值未作改变，则再次发送改变密钥通知和随机数或加密的新密钥，直到移动终端启用新的密钥进行通信。

由上可见，上述密钥分配方法并不涉及无线局域网内登录管理、认证管理和移动管理的特定方式，因此可以在各种无线局域网协议体系下实现，包括 PPPoE、IEEE 802.1x 协议等。但是为了进一步理解本发明的特点、优点和目标，以下以 IEEE 802.1x 协议为例描述本发明密钥分配方法的具体实现方式。

IEEE 802.1x 是一种常用的无线局域网的协议体系，涉及 MAC 层和物理层标准，AP 与移动终端之间的数据分组以 MAC 帧为单位。IEEE 802.1x 协议报文主要包括 EAP_START、EAP_LOGOOF、EAP_REQUEST、EAP_RESPONSE、EAP_SUCCESS、EAP_FAIL 和 EAP_KEY，这些报文为特殊的 MAC 帧，都通过 MAC 帧中的类型域来标识。

当移动终端与 AP 之间初始连接时，首先移动终端向 AP 发送 EAP_START 报文，AP 在收到后向移动终端发送 EAP_REQUEST/IDENTITY 报文，要求用

户输入用户名和密码。用户输入用户名和密码，移动终端将它们封装在 EAP_RESPONSE/IDENTITY 报文中并回送给 AP。AP 将用户提供的用户名和密码信息封装在 Access_Request 报文中发送给认证服务器，AP 与认证服务器之间的通信遵循 Radius 协议。认证服务器首先验证用户名和密码是否匹配，如果不匹配，则确定认证失败并将 Accept-Reject 报文回送给 AP。AP 收到后发送 EAP_FAIL 报文给移动终端，拒绝移动终端接入。如果认证成功，则认证服务器发送 Access_Accept 报文，同时在该报文的数据域中包含该用户的对应信息 P。AP 收到该消息后，如上述密钥分配方法所述，既可以根据某一密钥生成算法从对应信息 P 生成密钥并发送 EAP_SUCCESS 报文给移动终端，也可以用对应信息 P 加密生成的密钥然后借助 EAP_KEY 报文传送给移动终端。相应地，移动终端可根据同样的密钥生成算法从自己存储的对应信息 P 生成密钥或者用对应信息 P 解密接收到的密钥。接着，移动终端使用密钥对 MAC 帧数据进行加密并传送给 AP，同时在 MAC 帧中加入加密标识。帧体域由 IV 域、数据域和 ICV 域组成，特别是在 IV 域中包含了 2 个比特的 KeyID 域作为同步标志。比较好的是，当 MAC 帧未加密时，KeyID=0，当开始加密通信时，每次改变密钥，KeyID 都递增 1，即 KeyID=KeyID+1。如果 KeyID=3，则再次更新密钥时将 KeyID 重置为 1 而不是 0。因此首次加密 MAC 数据时，移动终端发出的 MAC 帧中的域 KeyID=1。AP 在收到 KeyID＝1 的 MAC 帧后，确定移动终端已启用新分配的密钥，于是就用前述生成的密钥解密 MAC 数据，并且转换为以太网格式向有线网络转发。如果 AP 在发送 EAP_KEY 报文后，发现移动终端上传的 MAC 帧中的 KeyID 域仍然为 0，则重发 EAP_SUCCESS 报文或者 EAP_KEY。

为了动态地更新通信密钥，AP 可以自移动终端登录起，定期(例如每隔 10 分钟)或不定期地发送 EAP_KEY 报文，通知移动终端修改密钥。在发送的 EAP_KEY 中，可选择包含生成密钥所用的随机数或者用当前密钥加密的新密钥。移动终端在收到该报文后，可以用相同的密钥生成方法从该随机数生成新密钥或者用当前密钥解密新的密钥。接着，移动终端用新密钥加密 MAC 数据，同时使 KeyID 取值为 KeyID＝2。AP 检测上传的 MAC 帧的 KeyID 域，如果 KeyID 保持不变，则继续使用当前密钥解密 MAC 数据，同时重发 EAP_KEY 报文。如果 KeyID 改变，则使用新密钥解密 MAC 数据。

权利要求

1.一种无线局域网加密密钥的分发方法，所述无线局域网包含一接入站(AP)和若干存储自身标识信息的移动终端，移动终端通过无线信道与 AP 通信，AP 与外部网络和对移动终端身份进行认证的认证装置连接，所述认证装置存储有各移动终端的标识信息，其特征在于所述方法包含如下步骤：

(1)移动终端向认证装置发送包含标识信息的认证请求以请求对其进行身份认证；

(2)认证装置根据认证请求中包含的标识信息对移动终端进行认证，如果认证失败，则经 AP 向移动终端发送拒绝接入消息；如果认证成功，则认证装置向 AP 发送与密钥有关的信息 M1，并且经 AP 向该移动终端发送包含允许接入通知信息的消息，如果该消息包含与密钥有关的信息 M2，则必须经过加密处理；

(3)AP 根据认证装置向其发送的与密钥有关的信息 M1 获得密钥，移动终端根据认证装置经 AP 向其发送的消息获得密钥。

2.如权利要求 1 所述的无线局域网加密密钥的分发方法，其特征在于所述信息 M1 为认证装置根据认证请求中包含的标识信息查找到的相应特征信息，AP 获得密钥的方式为根据密钥生成算法从所述特征信息生成密钥，而移动终端获得密钥的方式为在接收到 AP 转发的包含允许接入通知信息的消息后根据同一密钥生成算法从自身存储的所述特征信息生成密钥。

3.如权利要求 1 所述的无线局域网加密密钥的分发方法，其特征在于所述信息 M1 为认证装置根据认证请求中包含的标识信息查找到的相应特征信息，AP 获得密钥的方式为根据密钥生成算法生成密钥，所述信息 M2 为 AP 获得的密钥并以所述特征信息加密后连同允许接入通知信息一起发送给移动终端，移动终端获得密钥的方式为用所述特征信息对信息 M2 进行解密以获得密钥。

4.如权利要求 1 所述的无线局域网加密密钥的分发方法，其特征在于所述信息 M1 为认证装置根据密钥生成算法从与认证请求中包含的标识信息对应的特征信息生成的密钥，移动终端获得密钥的方式为在接收到允许接入通知信息后根据同一密钥生成算法从自身存储的所述特征信息生成密钥。

5.如权利要求 1 所述的无线局域网加密密钥的分发方法，其特征在于所述信息 M1 和 M2 为认证装置根据密钥生成算法从与认证请求中包含的标识信息对应的特征信息生成的密钥，所述信息 M2 以所述特征信息加密后连同允许接入通知信息发送给移动终端，移动终端获得密钥的方式为在接收到允许接入通知信息后以自身存储的所述特征信息对信息 M2 解密获得密钥。

6.如权利要求 1－5 中任意一项所述的无线局域网加密密钥的分发方法，其特征在于自 AP 接收到移动终端发送的用密钥加密的数据分组起定期或不定期地以包含如下步骤的方式更新密钥：

(a1)AP 产生一个随机数并利用任一密钥生成算法从该随机数生成新密钥；

(b1)AP 将该随机数放入改变密钥通知一起发送给移动终端；

(c1)当移动终端收到改变密钥通知后，根据改变密钥通知中包含的随机数，利用与步骤(a)中所述相同的密钥生成算法产生新密钥；

(d1)移动终端用新密钥对发送至 AP 的数据分组进行加密并向 AP 发送，在加密时移动终端在数据分组内加入加密标识并改变加密标识的数值以表示已经更换通信密钥；以及

(e1)AP 接收到移动终端发送的数据分组后，根据其中的加密标识的数值决定是否更换密钥。

7.如权利要求 1－5 中任意一项所述的无线局域网加密密钥的分发方法，其特征在于自 AP 接收到移动终端发送的用密钥加密的数据分组起定期或不定期地以包含如下步骤的方式更新通信密钥以完成新密钥下的加密通信：

(a2)AP 以任意方式生成新的密钥并用当前使用的密钥对新生成的密钥进行加密；

(b2)AP 将加密后的密钥放入改变密钥通知一起发送给移动终端；

(c2)当移动终端收到改变密钥通知后，用当前使用的密钥解密包含在改变密钥通知中的新密钥从而获得新密钥；

(d2)移动终端用新密钥对发送至 AP 的数据分组进行加密并向 AP 发送，在加密时移动终端在数据分组内加入加密标识并改变加密标识的数值以表示已经更换通信密钥；以及

(e2)AP 接收到移动终端发送的数据分组后，根据其中的加密标识的数值决定是否更换密钥。

8.如权利要求 1－5 中任意一项所述的无线局域网加密密钥的分发方法，其特征在于自 AP 接收到移动终端发送的用密钥加密的数据分组起定期或不定期地以包含如下步骤的方式更新密钥：

(a3)认证装置首先产生一个随机数以利用密钥生成算法从该随机数生成新密钥，然后将新密钥发送给 AP 而将随机数经 AP 发送给移动终端；

(b3)AP 在接收到新密钥之后将改变密钥通知发送给移动终端；

(c3)当移动终端收到认证装置发送的随机数和 AP 发送的改变密钥通知

后，根据随机数，利用与步骤(a)中所述相同的密钥生成算法产生新密钥；

(d3)移动终端用新密钥对发送至 AP 的数据分组进行加密并向 AP 发送，在加密时移动终端在数据分组内加入加密标识并改变加密标识的数值以表示已经更换通信密钥；以及

(e3)AP 接收到移动终端发送的数据分组后，根据其中的加密标识的数值决定是否更换密钥。

9.如权利要求 1－5 任意一项所述的无线局域网加密密钥的分发方法，其特征在于自 AP 接收到移动终端发送的用密钥加密的数据分组起定期或不定期地以包含如下步骤的方式更新通信密钥以完成新密钥下的加密通信：

(a4)认证装置以任意方式生成新的密钥并用当前使用的密钥对新生成的密钥进行加密，新密钥被发送给 AP 而加密后的新密钥经 AP 被发送给移动终端；

(b4)AP 接收到新密钥后向移动终端发送改变密钥通知；

(c4)当移动终端收到认证装置发送的加密密钥和 AP 发送的改变密钥通知后，用当前使用的密钥解密加密密钥从而获得新密钥；

(d4)移动终端用新密钥对发送至 AP 的数据分组进行加密并向 AP 发送，在加密时移动终端在数据分组内加入加密标识并改变加密标识的数值以表示已经更换通信密钥；以及

(e4)AP 接收到移动终端发送的数据分组后，根据其中的加密标识的数值决定是否更换密钥。

10.如权利要求 1－5 中任意一项所述的无线局域网加密密钥的分发方法，其特征在于所述认证装置为外部网络内部设置的认证服务器。

11.如权利要求 6 所述的无线局域网加密密钥的分发方法，其特征在于所述认证装置为外部网络内部设置的认证服务器。

12.如权利要求 7 所述的无线局域网加密密钥的分发方法，其特征在于所述认证装置为外部网络内部设置的认证服务器。

13.如权利要求 8 所述的无线局域网加密密钥的分发方法，其特征在于所述认证装置为外部网络内部设置的认证服务器。

14.如权利要求 9 所述的无线局域网加密密钥的分发方法，其特征在于所述认证装置为外部网络内部设置的认证服务器。

15.如权利要求 1－5 中任意一项所述的无线局域网加密密钥的分发方法，其特征在于所述认证装置为将外部网络与 AP 连接起来的无线网关。

16.如权利要求 6 所述的无线局域网加密密钥的分发方法，其特征在于所述认证装置为将外部网络与 AP 连接起来的无线网关。

17.如权利要求 7 所述的无线局域网加密密钥的分发方法，其特征在于所

述认证装置为将外部网络与 AP 连接起来的无线网关。

18.如权利要求 8 所述的无线局域网加密密钥的分发方法，其特征在于所述认证装置为将外部网络与 AP 连接起来的无线网关。

19.如权利要求 9 所述的无线局域网加密密钥的分发方法，其特征在于所述认证装置为将外部网络与 AP 连接起来的无线网关。

20.如权利要求 1－5 中任意一项所述的无线局域网加密密钥的分发方法，其特征在于所述认证装置包括无线网关和外部网络内部设置的认证服务器。

21.如权利要求 6 所述的无线局域网加密密钥的分发方法，其特征在于所述认证装置包括无线网关和外部网络内部设置的认证服务器。

22.如权利要求 7 所述的无线局域网加密密钥的分发方法，其特征在于所述认证装置包括无线网关和外部网络内部设置的认证服务器。

23.如权利要求 8 所述的无线局域网加密密钥的分发方法，其特征在于所述认证装置包括无线网关和外部网络内部设置的认证服务器。

24.如权利要求 9 所述的无线局域网加密密钥的分发方法，其特征在于所述认证装置包括无线网关和外部网络内部设置的认证服务器。

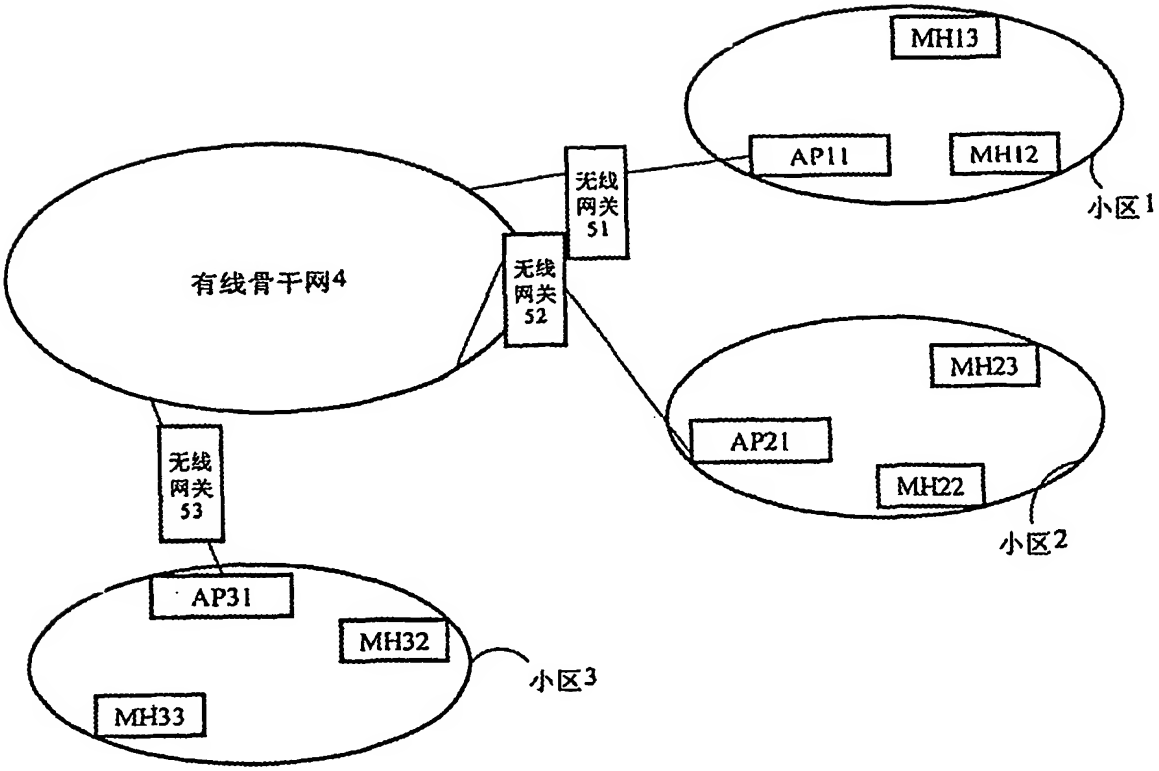

MH13
AP11
MH12
小区1
无线网关51
无线网关52
有线骨干网4
MH23
AP21
MH22
小区2
无线网关53
AP31
MH32
小区3
MH33

图 1

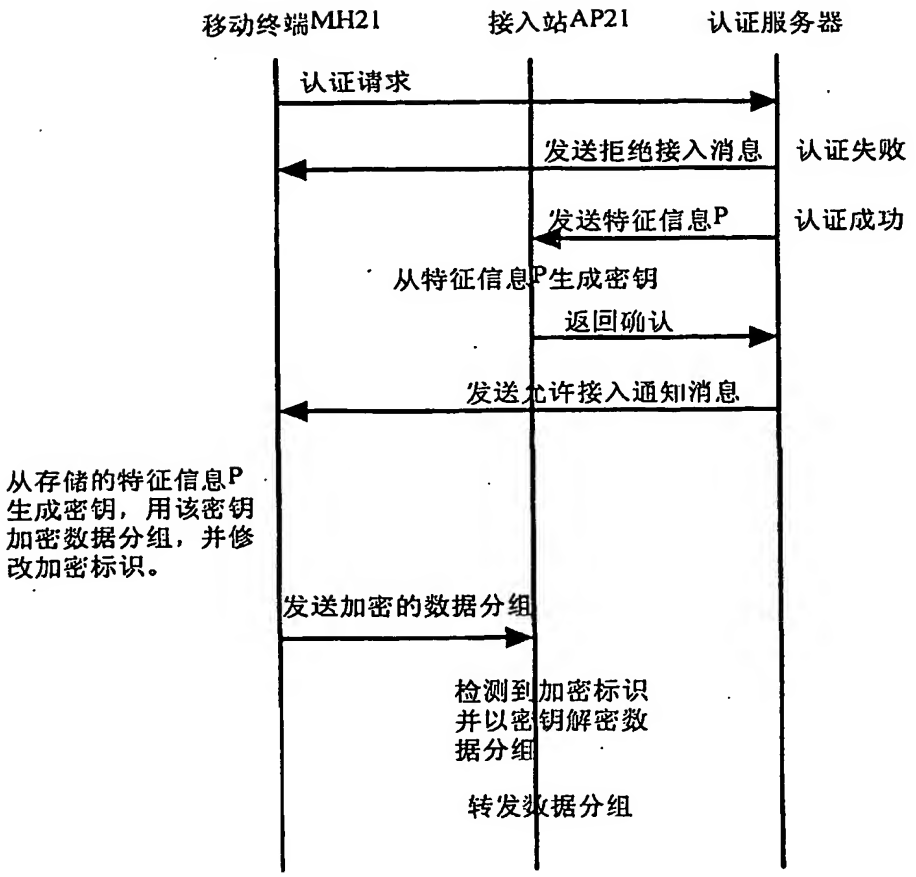

移动终端MH21
接入站AP21
认证服务器
认证请求
发送拒绝接入消息
认证失败
发送特征信息P
认证成功
从特征信息P生成密钥
返回确认
发送允许接入通知消息
从存储的特征信息P生成密钥，用该密钥加密数据分组，并修改加密标识。
发送加密的数据分组
检测到加密标识并以密钥解密数据分组
转发数据分组

图 2a

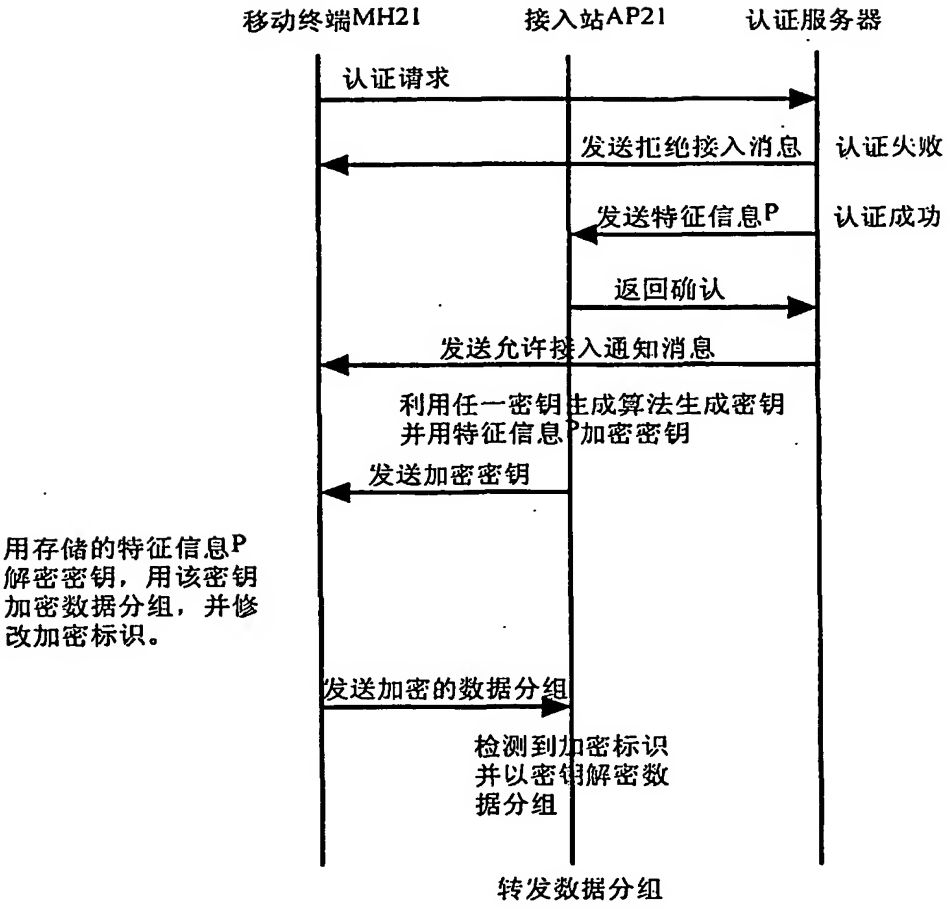

移动终端MH21
接入站AP21
认证服务器
认证请求
发送拒绝接入消息
认证失败
发送特征信息P
认证成功
返回确认
发送允许接入通知消息
利用任一密钥生成算法生成密钥
并用特征信息P加密密钥
发送加密密钥
用存储的特征信息P
解密密钥，用该密钥
加密数据分组，并修
改加密标识。
发送加密的数据分组
检测到加密标识
并以密钥解密数
据分组
转发数据分组

图 2b

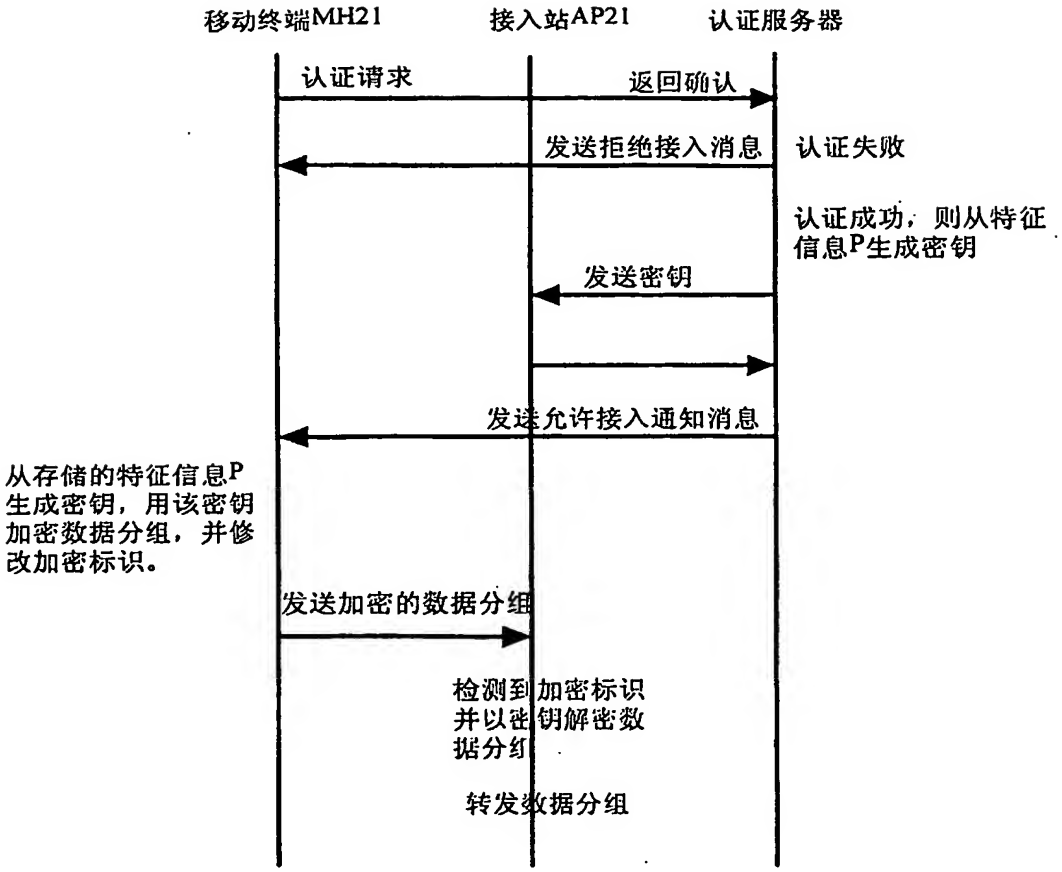

移动终端MH21
接入站AP21
认证服务器
认证请求
返回确认
发送拒绝接入消息
认证失败
认证成功，则从特征信息P生成密钥
发送密钥
发送允许接入通知消息
从存储的特征信息P生成密钥，用该密钥加密数据分组，并修改加密标识。
发送加密的数据分组
检测到加密标识
并以密钥解密数据分组
转发数据分组

图 2c

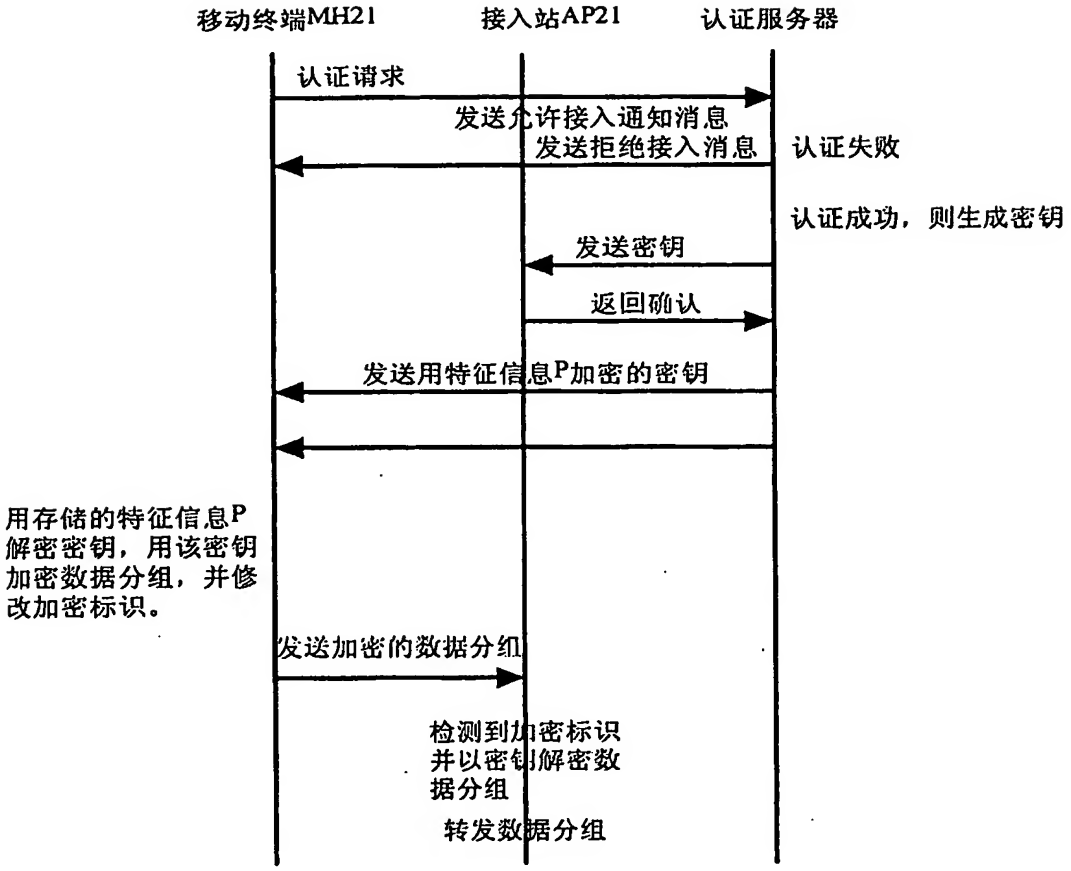

移动终端MH21
接入站AP21
认证服务器
认证请求
发送允许接入通知消息
发送拒绝接入消息
认证失败
认证成功，则生成密钥
发送密钥
返回确认
发送用特征信息P加密的密钥
用存储的特征信息P解密密钥，用该密钥加密数据分组，并修改加密标识。
发送加密的数据分组
检测到加密标识并以密钥解密数据分组
转发数据分组

图 2d

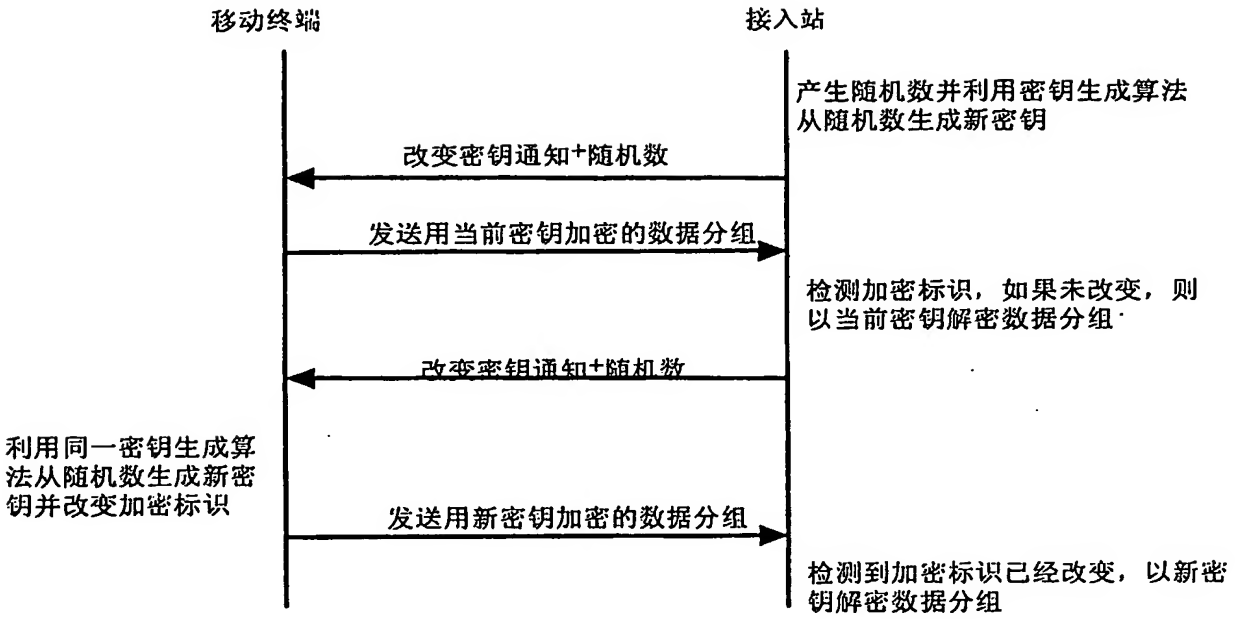

移动终端
接入站
产生随机数并利用密钥生成算法从随机数生成新密钥
改变密钥通知+随机数
发送用当前密钥加密的数据分组
检测加密标识，如果未改变，则以当前密钥解密数据分组
改变密钥通知+随机数
利用同一密钥生成算法从随机数生成新密钥并改变加密标识
发送用新密钥加密的数据分组
检测到加密标识已经改变，以新密钥解密数据分组

图 3a

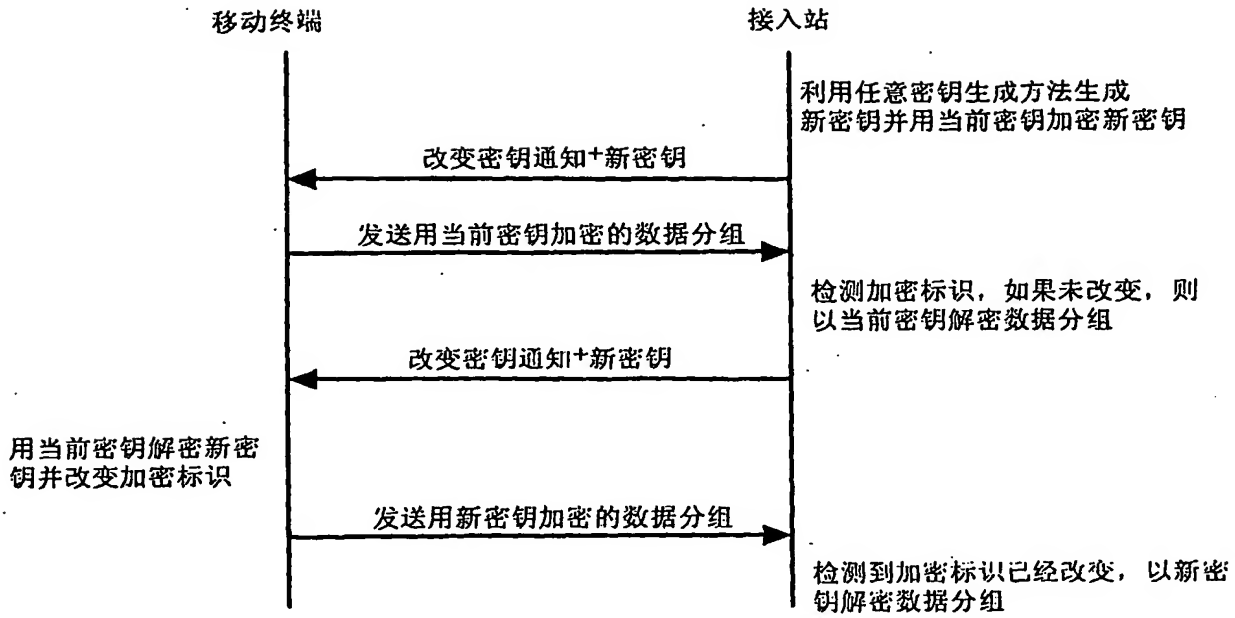

移动终端
接入站
利用任意密钥生成方法生成
新密钥并用当前密钥加密新密钥
改变密钥通知+新密钥
发送用当前密钥加密的数据分组
检测加密标识，如果未改变，则
以当前密钥解密数据分组
改变密钥通知+新密钥
用当前密钥解密新密
钥并改变加密标识
发送用新密钥加密的数据分组
检测到加密标识已经改变，以新密
钥解密数据分组

图 3b

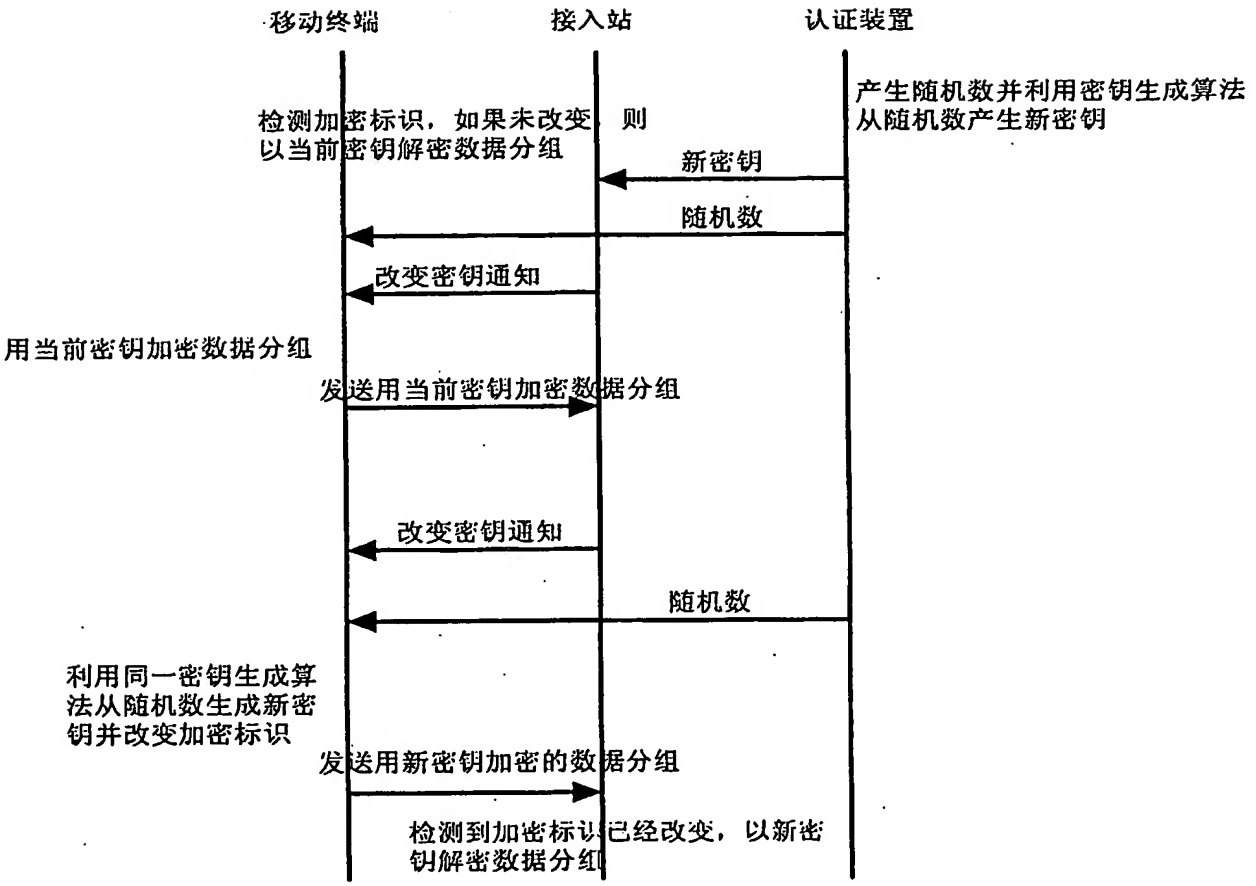

移动终端
接入站
认证装置
产生随机数并利用密钥生成算法从随机数产生新密钥
检测加密标识，如果未改变 则 以当前密钥解密数据分组
新密钥
随机数
改变密钥通知
用当前密钥加密数据分组
发送用当前密钥加密数据分组
改变密钥通知
随机数
利用同一密钥生成算法从随机数生成新密钥并改变加密标识
发送用新密钥加密的数据分组
检测到加密标识已经改变，以新密钥解密数据分组

图 3c

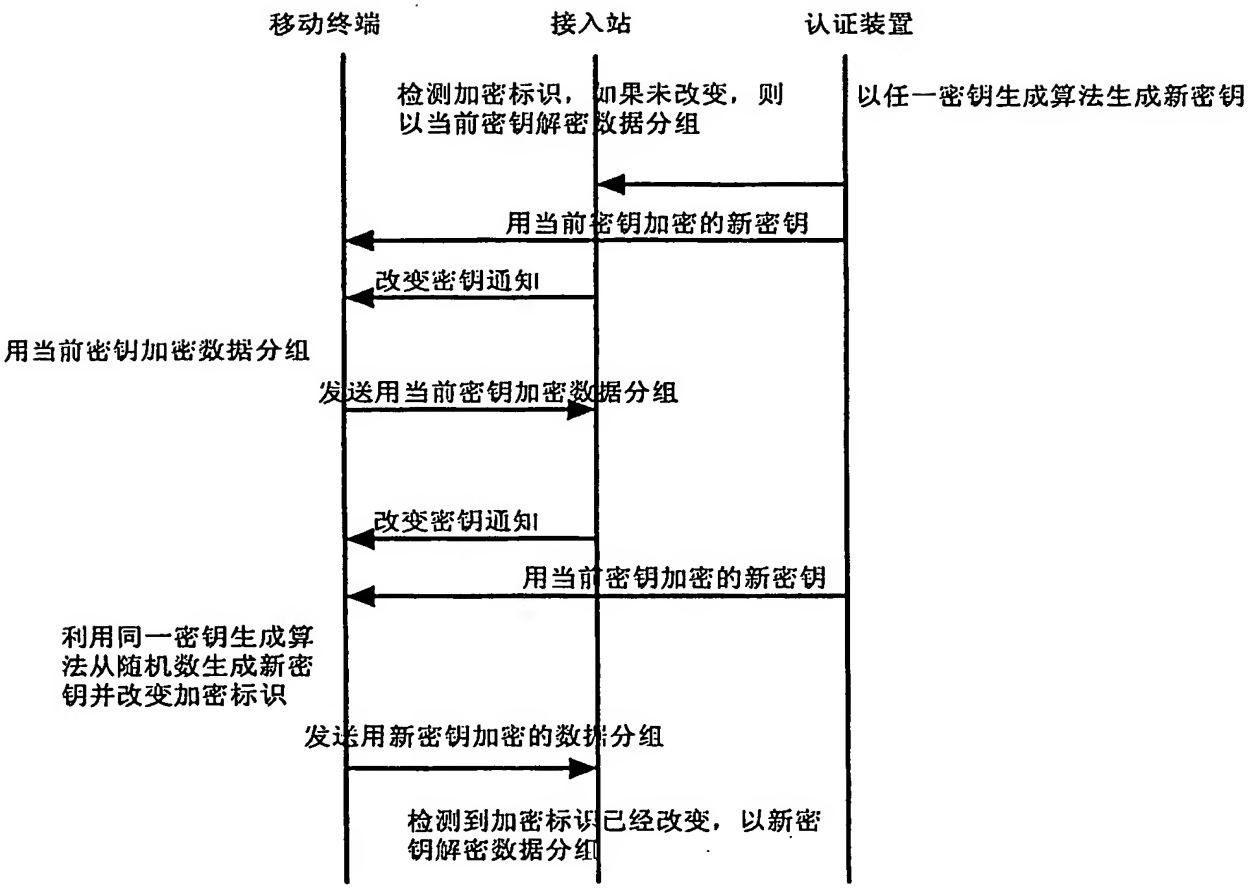

移动终端
接入站
认证装置
检测加密标识，如果未改变，则以当前密钥解密数据分组
以任一密钥生成算法生成新密钥
用当前密钥加密的新密钥
改变密钥通知
用当前密钥加密数据分组
发送用当前密钥加密数据分组
改变密钥通知
用当前密钥加密的新密钥
利用同一密钥生成算法从随机数生成新密钥并改变加密标识
发送用新密钥加密的数据分组
检测到加密标识已经改变，以新密钥解密数据分组

图 3d

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN03/00106

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04L9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, EPODOC, PAJ, CNPAT wireless LAN encrypt key distribute authentication mobile terminal manage

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP,A1,0658021, (International Business Machines Corporation) 14.June.1995(14.06.95) Whole document	1—24
A	JP,A,2001/244874 , (KENWOOD CORP) 07.September.2001(07.09.01) Whole document	1
A	CN,A,1264521, (ORANGE PERSONAL COMMUNICATIONS SERVICES) 23August.2000(23.08.00) Whole document	1

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22.April 22. 2003(22.04.03)	08 MAY 2003 (08.05.03)
Name and mailing address of the ISA/CN 6 Xitucheng Rd., Jimen Bridge, Haidian District, 100088 Beijing, China Facsimile No. 86-10-62019451	Authorized officer Li Zhen Hua Telephone No. 86-10-62093736

Form PCT/ISA /210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN03/00106

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP,A1,0658021	14.June.1995	US,A,5373078	13.Dec December.1994
		JP,A,7179764	18,July ,1995
		AU,A, 7751794	18.May.1995
JP,A,2001/244874	07.September.2001	WO,A,0165720	07.September.2001
CN,A,1264521	23August.2000	WO,A1,9904583	28.January.1999
		GB,A,2327567	27.January.1999
		EP,A1,0997047	03.May.2000
		AU,A,8348798	10. February.1999

国际检索报告

国际申请号 PCT/CN03/00106

A. 主题的分类

IPC7:H04L9/00

按照国际专利分类表(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类体系和分类号)

IPC7:H04L9/00

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称和，如果实际可行的，使用的检索词)

WPI，EPODOC，PAJ，CNPAT: wireless LAN encrypt key distribute authentication mobile terminal manage 无线局域网 加密 密钥 认证 移动终端 管理

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求编号
A	EP,A1,0658021，(国际商务机器有限公司) 14.6 月.1995(14.06.95) 全文	1—24
A	JP,A,2001/244874 ，(KENWOOD 有限公司) 07.9 月.2001(07.09.01) 全文	1
A	CN,A,1264521，(奥林吉个人通讯服务公司）23.8 月.2000(23.08.00)全文	1

☐ 其余文件在 C 栏的续页中列出。

☒ 见同族专利附件。

* 引用文件的专用类型：

"A" 明确叙述了被认为不是特别相关的一般现有技术的文件

"E" 在国际申请日的当天或之后公布的在先的申请或专利

"L" 可能引起对优先权要求的怀疑的文件，为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布的在后文件，它与申请不相抵触，但是引用它是为了理解构成发明基础的理论或原理

"X" 特别相关的文件，仅仅考虑该文件，权利要求所记载的发明就不能认为是新颖的或不能认为是有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，权利要求记载的发明不具有创造性

"&" 同族专利成员的文件

国际检索实际完成的日期	国际检索报告邮寄日期
22.4 月 2003(22.04.03)	08. 5月 2003 (08.05.03)
国际检索单位名称和邮寄地址 ISA/CN 中国北京市海淀区西土城路 6 号(100088) 传真号： 86-10-62019451	受权官员 李振华 电话号码：86-10-62093786

国际检索报告
关于同族专利成员的情报

国际申请号
PCT/CN03/00106

检索报告中引用的专利文件	公布日期	同族专利成员	公布日期
EP,A1,0658021	14.6 月.1995	US,A,5373078	13,12 月.1994
		JP,A,7179764	18,7 月,1995
		AU,A, 7751794	18.5 月.1995
JP,A,2001/244874	07.9 月.2001	WO,A,0165720	07.9 月.2001
CN,A,1264521	23.8 月.2000	WO,A1,9904583	28.1 月.1999
		GB,A,2327567	27.1 月.1999
		EP,A1,0997047	03.5 月.2000
		AU,A,8348798	10.2 月.1999